ATTACHMENT 1

PERFORMANCE WORK STATEMENT (PWS)

DEPARTMENT OF VETERANS AFFAIRS (VA)
VETERANS HEALTH ADMINISTRATION (VHA)

Health Information Management Office (HIM)
Office of Health Information (OHI)
Enterprise-wide Front-end Speech Recognition Purchase
Date: 04/11/2013 version 2

Contents

1.0 BACKGROUND

A central goal of VA is to ensure the highest level of patient care to our nation's Veterans. A keystone to quality patient care is accurate, timely and complete medical documentation. The majority of Veterans Health Administration's (VHA) clinical documentation resides in the Computerized Patient Record System (CPRS); the VA's highly regarded electronic health record (EHR). There are a variety of methods of medical documentation entry including manual entry, third-party transcription, and limited usage of speech recognition software. Currently, the primary speech recognition software used by non-radiologists is Nuance's Dragon Medical.

To ensure the continuation of high-quality and well-documented patient care, VHA seeks to purchase a Medical-Specific Enterprise-wide Front-End Speech Recognition System for non-Radiology applications. VHA holds approximately 7,000 Nuance Dragon Medical licenses, including a variety of versions (i.e., Versions 6.10.x – 10.1.x,). In establishing an enterprise-wide system, VHA seeks to standardize their approach to non-Radiology speech-recognition software, as well as maintain the most current version of the chosen software across all VHA facilities. It is anticipated that optimizing an enterprise-wide system will improve productivity and user satisfaction of clinicians, reduce costs of transcription, improve accuracy and quality of medical documentation, and ultimately enhance patient-centered care. The system will help with sharing best practices, achieving operational efficiencies, and leveraging economies of scale.

Although VA presently utilizes approximately 7,000 individual Speech Recognition licenses, this amount is projected to increase to at least 12,000 licenses for traditional users utilizing speech recognition from a traditional workspace such as a desktop or laptop over the next five years. The need for medical specific speech recognition software via mobile devices is anticipated to grow significantly over the next five years; no projections for increase are currently available as VHA's healthcare team-facing mobile platform is still under development.

2.0 APPLICABLE DOCUMENTS

Documents referenced or germane to this PWS are listed below. In the performance of the tasks associated with this PWS, the Contractor shall comply with the following:

1. 44 United States Code (U.S.C.) § 3541, "Federal Information Security Management Act (FISMA) of 2002"
2. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
3. FIPS Pub 201, "Personal Identity Verification of Federal Employees and Contractors," March 2006
4. 10 U.S.C. § 2224, "Defense Information Assurance Program"
5. Software Engineering Institute, Software Acquisition Capability Maturity Model (SA CMM) Level 2 procedures and processes
6. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"
7. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"

8. VA Directive 0710, “Personnel Suitability and Security Program,” September 10, 2004
9. VA Directive 6102, “Internet/Intranet Services,” July 15, 2008
10. 36 Code of Federal Regulations (C.F.R.) Part 1194 “Electronic and Information Technology Accessibility Standards,” July 1, 2003
11. Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources,” November 28, 2000
12. 32 C.F.R. Part 199, “Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)”
13. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005
14. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
15. Homeland Security Presidential Directive (12) (HSPD-12)
16. VA Directive 6500, “Information Security Program,” August 4, 2006
17. VA Handbook 6500, “Information Security Program,” September 18, 2007
18. VA Handbook, 6500.5, Incorporating Security and Privacy in System Development Lifecycle.
19. VA Handbook 6500.6, “Contract Security,” March 12, 2010
20. Project Management Accountability System (PMAS) portal (reference PWS References -Technical Library at https://www.voa.va.gov/)
21. Office of Enterprise Development (OED) ProPath Process Methodology (reference PWS References -Technical Library and ProPath Library links at https://www.voa.va.gov/) NOTE: In the event of a conflict, OED ProPath takes precedence over other processes or methodologies.
22. Technical Reference Model (TRM) (reference at http://www.ea.oit.va.gov/Technology.asp)
23. National Institute Standards and Technology (NIST) Special Publications
24. VA Office of Inspector General (OIG) Audit of VHA’s Acquisition of Medical Transcription Services (http://www.va.gov/oig/52/reports/2006/VAOIG-04-00018-155.pdf)

3.0 SCOPE OF WORK

The objective of this Performance Work Statement (PWS) is to support the VHA’s ability to acquire, implement and integrate an Enterprise-wide Front-end Speech Recognition System. The scope of this effort includes:

1. Licensing, Hardware & Software System
2. Implementation Support and Ongoing Maintenance
3. Training

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance is one (1) base year and four (4) option years from the date of award.

With the exception of major system failure, any work at a Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO). A major system failure includes network down, power outage, data center down, and identified servers for product installation being down.

There are 10 Federal holidays set by law (U.S.C. Title 5 Section 6103) that the VA follows:

Under current definitions, four (4) are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six (6) are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

The work shall take place at the vendor’s site and various VHA facilities listed in Attachment A.

4.3 TRAVEL AND PER DIEM

Travel and per diem shall be reimbursed in accordance with VA/Federal Travel Regulations.

Travel to VA facilities may be required at times to complete engagements. Specific travel requirements will be specified within an individual Task Order. Currently there are approximately 1,300 VHA facilities across the United States (U.S.) and the Republic of the Philippines. The U.S. is defined as the 50 States, Territories and possessions, the District of Columbia, the Commonwealth of Puerto Rico, and the

Commonwealth of the Northern Mariana Islands. Performance may take place at any VHA facilities listed on the following web site:

http://www2.va.gov/directory/guide/Allstate_flsh.asp?dnum=1
(Note: Sites subject to updates as VA facility changes are implemented.)

Reimbursement of travel expenses are allowable only to the extent authorized on the individual Task Order. Additionally, the VA Program Manager (PM) and Contracting Officer's Representative (COR) must approve all travel requirements/requests before travel begins. Travel that occurs without pre-approval by the COR will NOT be reimbursed. The Contractor submits a Travel Request Form (Attachment C) no later than 10 days prior to the commencement of travel. Travel and per diem expenses will be reimbursed on an actual expenditures basis in accordance with the Federal Travel Regulations (FTR) and Federal Acquisition Regulation (FAR) Part 31.205-46. In order to be reimbursed for travel, the Contractor shall submit supporting documentation as required by FTR with invoices. FTR require receipts for travel expenditures of $75.00 or more. Expenses for subsistence and lodging will be reimbursed to the Contractor only to the extent where an overnight stay is necessary and authorized by FTR in effect at a time of the stay for the specific locations.

VA anticipates travel will be required primarily for training purposes. Training will take place in at least the initial pilot site, Training may also occur at centralized VISN locations, and one Pilot site. The table below represents the estimated travel for the base and option years for work to be performed.

Estimated Locations	Approximate # of trips per contract year	Approximate # Contractor Personnel per trip	Approximate # days per trip
Bedford, MA	2	2	5
*Boston, MA	2	2	5
Albany, NY	2	2	5
Bronx, NY	2	2	5
Pittsburgh, PA	2	2	5
Linthicum, MD	2	2	5
Washington, DC	2	2	5
Durham, NC	2	2	5
Duluth, GA	2	2	5
St. Petersburg, FL	2	2	5
Nashville, TN	2	2	5

Cincinnati, OH	2	2	5
Ann Arbor, MI	2	2	5
Hines, IL	2	2	5
Kansas City, MO	2	2	5
Ridgeland, MS	2	2	5
Arlington, TX	2	2	5
Mesa, AZ	2	2	5
Glendale, CO	2	2	5
Vancouver, WA	2	2	5
Mare Island, CA	2	2	5
Long Beach, CA	2	2	5
Minneapolis, MN	2	2	5

*Pilot Site

5.0 FUNCTIONAL TASK AREAS

5.1 ENTERPRISE-WIDE FRONT-END SPEECH RECOGNITION SYSTEM

The Contractor shall provide medical-specific front-end speech recognition software, licenses, server hardware, storage and peripherals.

The software shall be customizable by medical specialty. The system shall work in a centralized, virtual environment behind the VA firewall to allow regionally-consolidated storage and management, as defined by VA OIT (see Attachment B). Additionally, this system shall have the technical capabilities to:

a) Interface with the Commercial Off-the-Shelf (COTS) products deployed within VHA (e.g., Microsoft Office Suite Version 2007 and 2010, VA Secure Messaging Systems,) and CPRS (or the current interface for VHA electronic health records);

b) Interface with a variety of microphones to accommodate user needs; peripheral input devices shall have noise cancelling capabilities and shall be compatible with speech recognition software.

c) Operate in roaming mode within a facility such that VA clinicians can dictate from any available work station;

d) Be accessed through VA's remote access solutions (e.g., RESCUE Virtual Private Network (VPN), Citrix Access Gateway,);

e) Make at least basic medical-specific speech recognition features available to clinicians via a mobile device, such as a smartphone or tablet running iOS or Android.

f) Provide concurrent use; and

g) Operate in a Citrix, “thin client,” environment.

The system shall also enhance the user-experience through its ability to:

a) Create user-specified, voice-enabled customized commands;

b) Accommodate varying accents of spoken English;

c) Provide pre-determined VA specified terms and acronyms in user's vocabulary, customizable at the facility and user levels;

d) Pre-populate software with VA provided, CPRS-specific voice enabled commands; and

e) Utilize the speech recognition software to correct errors in accuracy.

Deliverables

A. Front-end Speech Recognition Unlimited Software Licenses.
B. Front-end Speech Recognition Microphones.
C. Front-end Speech Recognition Server/Hardware.

5.2 IMPLEMENTATION SUPPORT

The Contractor shall provide strategies to transition from the current state of speech recognition technology to a centralized and unified state.

5.2.1 PRE-IMPLEMENTATION

It is expected the contractor will, in accordance with VA OIT policies to be provided at time of award, install all server and storage hardware. Additionally, the contractor is expected to ***manually install*** client software on a small subset of VA provided workstations, during the pilot phase, to validate compatibility and functionality of client software. The contractor, in concert with VA OIT, may leverage the VA's System Center Configuration Manager (SCCM) environment to deploy client software on a larger scale.

If, during the initial pilot phase, the software proposed does not properly operate on the VA's IT platform the Government reserves the right to terminate.

Deliverables

A. Transition Plan
B. Pre-Installation Brief
C. Project Management Plan
D. Implementation and Installation Plan

*The finalized plans shall be submitted 30 days after contract award and shall be updated, as applicable, during performance.

5.2.2 IMPLEMENTATION

The Contractor shall assist in implementing the Enterprise-wide Front-end Speech Recognition System. The Contractor shall successfully implement its proposed system in a phased approach. At a minimum, the phased approach shall address how to mitigate the following:

a) Disruption to VA end-users;
b) Disruption to facility IT systems; and
c) Unscheduled system downtime.

Implementation includes installation and configuration of the servers, workstations, client applications, and the interface of the speech recognition system with VA applications, including CPRS. The Contractor shall provide support to assist the Government in validating the operability of the Enterprise-wide Front-end Speech Recognition System during the testing phase.

During initial implementation, the Contractor shall provide daily reports and shall provide weekly reports until all sites are implemented.

During the initial Implementation/Pilot Phase the Daily Report shall include:

a) Regional Data Center – Schedule of hardware and software installations, progression of installations, identification of delays and/or issues, resolution of issues, time frame for resolution and best practices.

b) VHA Facility – Schedule of software installations, progression of installations, identification of delays and/or issues, resolution of issues, time frame for resolution and best practices.

The Weekly Reports shall include:

a) Regional Data Center – Installation of hardware and software is proceeding as scheduled and any issues are identified, resolution has been identified and time frame for resolution and best practices

b) VHA Facility – Progression of software installation at provider's site, issues are identified, resolution has been identified time frame for resolution and best practices

After the initial site installations, the Contractor shall provide an Installation "Cook Book" to be used by region, VISN, and/or facility OIT staff for facility level deployments. The "CookBook" will detail proven technical installation instructions, procedures, and lessons learned used in the successful migration of those sites. This Installation "Cook Book" shall ensure the process is seamless and easily replicated in all VHA facilities.

Deliverables

A. Installation "Cook Book"
B. Initial Installation Daily Reports
C. Weekly Reports

5.2.3 Post Implementation

After installation, the Contractor shall provide personnel at the pilot facilities to test the speech recognition system and mitigate any issues. The Contractor shall also deliver a post implantation brief to VHA and OIT personnel that contains the following:

a) Summary of all issues;

b) Resolution of issues;

c) Testing results;

d) Lessons Learned/Best Practices; and

e) Recommendations for proceeding.

Deliverables

A. Post-Implementation Brief

5.3 ONGOING MAINTENANCE

5.3.1 Maintenance and Support

The Contractor shall provide Enterprise-wide Front-end Speech Recognition System maintenance and support (e.g., software updates, patches, current versions,). Downtime for system upgrades shall occur outside of normal business hours and shall not exceed two (2) hours per month. Under the rare circumstance that an upgrade takes longer than scheduled by 30 minutes, VA must be notified of exception and contractor must develop mitigation strategy to ensure continuity of services.

When Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the systems within 10 working days of release of third party security update or software patch. The vendor is responsible for operations or maintenance of the System and shall either apply the Security Fixes or software patches within 30 days or provide to the government a package that contains the Security Fixes or software patches for installation by the government with vendor support.

Contractor shall notify the VA of any material errors or defects in the Software known, or made known to Contractor from any source during the term of this Agreement that could cause the production of inaccurate, or otherwise materially incorrect, results. Contractor shall initiate actions to remediate errors or defects within 5 (five) business days of error or defect becoming known to the Contractor.

The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved Federal Desktop Core Configuration (FDCC).

Deliverables

A. Maintenance and Support Strategic Plan
B. Maintenance and Support

*The finalized plan shall be submitted 30 days after contract award and shall be updated, as applicable, during performance.

5.3.2 Customer Service

The Contractor shall provide 24/7/365 Tier 2 system support throughout the PoP. Any telephonic help desk support shall be provided at no additional cost. The Contractor shall respond to trouble tickets within two (2) hours of the initial request.

The Contractor shall provide VA with a monthly summary report of helpdesk activity. This summary shall include the date and time of inquiry, the user's name and facility, a brief summary of the inquiry, a brief summary of the resolution, and any deviation from required response time and rationale.

The Contractor will provide at least normal and usual software support and maintenance services generally provided to customers in a similar program, position or setting with and subject to the payment of the support and maintenance fees agreed upon in this Contract.

Deliverables

A. User support summary report

5.4 TRAINING

Administrator training shall instruct facility administrators on how to perform daily maintenance and operations of the system. Administrator training shall include:

a) Demonstration of Disaster Recovery/Continuity of Operations Plan;

b) Back-up and recovery procedures;

c) System optimization strategy and procedures;

d) Installation procedures for updates, upgrades, and patches; and

e) Peripherals (e.g., microphones,) management procedures.

The Contractor shall provide virtual/web-based training, instructional handouts/manuals, quick reference guides, train the trainer strategies and manuals, and direct classroom training.

The Contractor shall ensure all existing and new end-users can demonstrate proficient use of the Enterprise-wide Front-end Speech Recognition System and associated peripherals. The Contractor shall assist VA in defining a minimum standard of system proficiency. Historically, VA has a subset of users who underutilize speech recognition technology. Accordingly, the Contractor shall provide cost-effective and efficient strategies to optimize user proficiency. Contractor-provided training materials shall be the property of the Government, readily available to VA staff, easily reproduced, and accessible in a common format.

Deliverables

A. Training Plan
B. Training

*The finalized plan shall be submitted 30 days after contract award and shall be updated, as applicable, during performance.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OIT Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directive issued by the Office of Management and Budget (OMB) on September 28, 2010 (http://www.cio.gov/documents/IPv6memofinal.pdf). IPv6 technology, in accordance with the USGv6 Profile (NIST Special Publication (SP) 500-267, http://www.antd.nist.gov/usgv6/) and NIST SP 800 series applicable compliance, shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. All public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) shall support native IPv6 users and all internal infrastructure and applications shall operate using native IPv6. To ensure interoperability, IPv4 will coexist during the transition to IPv6 and it is expected that VA will continue running IPv4 until it is phased out by 2015. By 2015, all computing, application, and network resources must turn off IPv4 as a communication mechanism in VA, unless a waiver is obtained from the Office of the Principal Deputy Assistant Secretary for Information and Technology, Department of Veterans Affairs or the device/service runs in an enclave.

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 9 and Microsoft Office 2010. However, the migration from Windows XP to Windows 7 is not yet complete within all of VA. As a result, compatibility with and support on Windows XP, Internet Explorer 7 and Microsoft Office 2007 are also required until April 2014 when Microsoft's extended support for Windows XP ends. In addition, the Contractor IT solution shall be deployable using System Center Configuration Manager (SCCM) tool.

The Contractor shall support VA efforts in accordance with the Project Management Accountability System (PMAS) that mandates all new VA IT projects/programs use an incremental development approach, requiring frequent delivery milestones that deliver new capabilities for business sponsors to test and accept functionality. Implemented by the Assistant Secretary for IT, PMAS is a VA-wide initiative to better empower the OIT Project Managers and teams to meet their mission: delivering world-class IT products that meet business needs on time and within budget.

The Contractor shall utilize ProPath, the OIT-wide process management tool that assists in the execution of an IT project (including adherence to PMAS standards). It is a one-stop shop providing critical links to the formal approved processes, artifacts, and templates to assist project teams in facilitating their PMAS-compliant work. ProPath is used to build schedules to meet project requirements, regardless of the development methodology employed.

6.2 POSITION RISK DESIGNATION LEVEL(S) AND CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Position Sensitivity	**Background Investigation** (in accordance with Department of Veterans Affairs 0710 Handbook, "Personnel Security Suitability Program," Appendix A)
Low	**National Agency Check with Written Inquiries (NACI)** A NACI is conducted by OPM and covers a 5-year period. It consists of a review of records contained in the OPM Security Investigations Index (SII) and the DOD Defense Central Investigations Index (DCII), FBI name check, FBI fingerprint check, and written inquiries to previous employers and references listed on the application for employment. In VA it is used for Non-sensitive or Low Risk positions.
Moderate	**Moderate Background Investigation (MBI)** A MBI is conducted by OPM and covers a 5-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check], a credit report covering a period of 5 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, law enforcement check; and a verification of the educational degree.
High	**Background Investigation (BI)** A BI is conducted by OPM and covers a 10-year period. It consists of a review of National Agency Check (NAC) records [OPM Security Investigations Index (SII), DOD Defense Central Investigations Index (DCII), FBI name check, and a FBI fingerprint check report], a credit report covering a period of 10 years, written inquiries to previous employers and references listed on the application for employment; an interview with the subject, spouse, neighbors, supervisor, co-workers; court records, law enforcement check, and a verification of the educational degree.

The Tasks identified below and the resulting Position Sensitivity and Background Investigation delineate the Background Investigation requirements by Contractor individual, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each individual, based upon the tasks the Contractor individual will be working, based upon their submitted proposal.

6.2.1 LOW RISK DESIGNATION TASKS

The position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the Performance Work Statement are:

	Position Sensitivity and Background Investigation Requirements		
Task Number	Low/NACI	Moderate/MBI	High/BI
5.1	X	☐	☐
5.2	X	☐	☐
5.3	X	☐	☐
5.4	X	☐	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working.

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working.

6.2.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak and understand the English language.
b. The Contractor shall bear the expense of obtaining background investigations.
c. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations. The roster shall contain the Contractor's Full

Name, Full Social Security Number, Date of Birth, Place of Birth, and individual background investigation level requirement (based upon Section 6.2 Tasks).

d. The Contractor should coordinate the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized.
e. For a Low Risk designation the following forms are required to be completed: 1.OF-306 and 2. DVA Memorandum – Electronic Fingerprints. For Moderate or High Risk the following forms are required to be completed: 1. VA Form 0710 and 2. DVA Memorandum – Electronic Fingerprints. These should be submitted to the COR within 5 business days after award.
f. The Contractor personnel will receive an email notification from the Security and Investigation Center (SIC), through the Electronics Questionnaire for Investigations Processes (e-QIP) identifying the website link that includes detailed instructions regarding completion of the investigation documents (SF85, SF85P, or SF 86). The Contractor personnel shall submit all required information related to their background investigations utilizing the Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP).
g. The Contractor is to certify and release the e-QIP document, print and sign the signature pages, and send them to the COR for electronic submission to the SIC. These should be submitted to the COR within 3 business days of receipt of the e-QIP notification email.
h. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
i. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC) or "Closed, No Issues" (SAC) finger print results, training delineated in VA Handbook 6500.6 (Appendix C, Section 9), and, the signed "Contractor Rules of Behavior." However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of the Office of Personnel Management (OPM).
j. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
k. Failure to comply with the Contractor personnel security investigative requirements may result in termination of the contract for default.

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include:

MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS:

The Contractor shall monitor performance against the established schedule, milestones, risks and resource support outlined in the approved PMP. As a minimum, the following metrics shall be included:

Required Service	Performance Standard	Acceptable Level	Surveillance Method
Adherence to Phased Implementation/Schedule	1. Contractor shall meet agreed upon milestones for phased implementation, installation and upgrades of speech recognition software. 2. Contractor shall meet agreed upon milestones for the training of new and existing users. 3. Contractor shall ensure that training and installation/upgrade of software occurs simultaneously and in accordance with the agreed phased implementation approach so that users may be able to operate software upon installation. 4. Contractor shall meet agreed to draft deliverables deadlines which allow for an internal review of the document before the Contractor's initial submission to the COR.	1. Scheduled deadlines are met 97% of the time. 2. Scheduled deadlines are met 97% of the time. 3. Scheduled deadlines are met 97% of the time. 4. Draft deliverables are received one (1) week before submission to the COR 97% of the time.	100% Inspection
Quality of Deliverables	1. Contractor shall provide clear, comprehensive, and accurate draft deliverables that meet all specified needs and require minimal to no Government edits for final acceptance. 2. Contractor's recommendations are comprehensive, valuable, and include in-depth benefit analysis that identifies areas of improvement and integration of best practices to Speech Recognition. 3. Contractor's presentations shall be clear,	1. Deliverables meet all specified quality, content, and format requirements and may be accepted as final by the Government with no more than two (2) review cycles 97% of the time. 2. Recommendations and in-depth benefit analyses are adequate, correct, and meet Customer	Random Sample

Required Service	Performance Standard	Acceptable Level	Surveillance Method
	concise, executive-focused, and written in plain, clear English with minimal jargon, understandable by lay persons.	needs, while adhering to industry's best practices 97% of the time 3. Presentations address all Speech Recognition needs clearly and concisely 97% of the time.	
Communications	1. Contractor shall manage the lines of communication between Speech Recognition customers, the sponsor, Contractor employees and other relevant third party vendors/parties in a professional, accurate and timely fashion. 2. Contractor shall address the requests and concerns of Speech Recognition customers. The Contractor's communication approach shall maintain a courteous environment for concerns to be properly addressed. Complaints pertaining to Contractor's communication approach shall be mitigated immediately. 3. Contractor shall collaborate seamlessly with third party vendors, when required, ensuring minimal disruption to normal work flow and efficiency.	1. All relevant parties are informed of all necessary factors throughout the duration of the project 100% of the time. Necessary follow-up communication about the status of an issue (and/or its resolution) occurs within 1 business day of initial request 97% of the time. 2. Government receives no repeat complaints pertaining to the Contractor's communication approach from stakeholders, Speech Recognition customers, or third parties. 3. Efforts requiring collaboration with third party vendors shall be executed successfully without the need of Government mediation 97% of the time.	Customer Complaints
Software	1. Software shall be available while VA network access is functional. 2. Contractor shall provide licensing.	1. 99.9% software availability with VA network access during initial implementation of post-install. 99% software availability with	1. Random Sample and Validated Customer Complaints 2. 100% Inspection of licensing if anything other

Required Service	Performance Standard	Acceptable Level	Surveillance Method
		VA network access 2. All licenses received.	than unlimited perpetual
Configuration Management	1. Provides specifications and configurations information for hardware and software components.	1. All hardware and software requirements are clearly defined including, Client/Server compatibility, COTS compatibility, and interfaces w/VA specific software.	100% Inspection
Training	1. Contractor shall provide training materials which are clear, concise and written in plain, clear English with minimal jargon, understandable by lay persons. 2. Contractor shall administer a user training survey upon completion of each on-site training session. The survey shall include questions concerning the following: Did the training add value, were users satisfied with the training, were skills in using software have improved because of the training, effectiveness of the trainer and their ability to communicate complex ideas, knowledge of the product , the user's confidence with using the product and/or teaching others how to use the product , any suggestions pertaining to what the contractor did well and how the training could be improved and an open comment field to address items that have not been included elsewhere in the survey.	1. 100% Training materials meet all specified quality, content, and format requirements and may be accepted as final by the Government. On-site training will meet all specified quality and content. 2. Overall average rating amongst all users of no less than three (3) on a five (5) point scale.	1. 100% Inspection 2. Validated Customer Complaint Random Sample of User Training Feedback Questionnaires to review ratings and comments fields.

The Government will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract/order to ensure that the Contractor is performing the services required by this PWS in an acceptable manner. The Government reserves the right to alter or change the QASP at its own discretion. A Performance Based Service Assessment Survey will be used in combination with the QASP to assist the Government in determining acceptable performance levels.

6.5 FACILITY/RESOURCE PROVISIONS

The Government shall provide office space, telephone service and system access when authorized contract staff work at a Government location as required in order accomplishing the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government COR. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

The VA shall provide access to VA specific systems/network as required for execution of the task via a site-to-site VPN or other technology, including VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, ProPath, Primavera, and Remedy, including appropriate seat management and user licenses. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. For detailed Security and Privacy Requirements refer to.

Addendum A and ADDENDUM B.

7.0 ACRONYMS

Acronym	Definition
ASD	Architecture, Strategy, and Design
ATO	Authority to Operate
AV	Antivirus
C&A	Certification and Accreditation
C.F.R.	Code of Federal Regulations
CHAMPUS	Civilian Health and Medical Program of the Uniformed Services
CO	Contracting Officer
COR	Contracting Officer's Representative
COTS	Commercial-off-the-Shelf
CPRS	Computerized Patient Record System
CPU	Central Processing Unit
CSCA	Contractor Security Control Assessment
DCII	Defense Central Investigations Index
DISCO	Defense Industrial Security Clearance Organization
DoD	Department of Defense
DSS	Defense Security Service
EA	Enterprise Architecture
EES	Employee Education System
EHR	Electronic Health Record
EIT	Electronic and Information Technology
EPHI	Electronic Protected Health Information
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigations
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only
FTR	Federal Travel Regulations
GFE	Government Furnished Equipment
GOE	Government Owned Equipment
HIPAA	Health Insurance Portability and Accountability Act
HSPD-12	Homeland Security Presidential Directive (12)
HVAC	Heating, Ventilation, Air Conditioning
ISO	Information Security Officer
MOU-ISA	Memorandum of Understand-Interconnection Service Agreement

Acronym	Definition
NAC	National Agency Check
NARA	National Archives and Records Administration
NISP	National Industrial Security Program
NIST	National Institute Standards and Technology
OE	Other Equipment
OED	Office of Enterprise Development
OHI	Office of Health Information
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PM	Program Manager
PMAS	Program Management Accountability System
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMP	Project Management Plan
POA&M	Plan of Action and Milestones
POC	Point of Contact
PoP	Period of Performance
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
SA CMM	Software Acquisition Capability Maturity Model
SIC	Security and Investigation Center
SII	Security Investigations Index
SOR	Systems of Records
SP	Special Publications
SSP	System Security Plans
TRM	Technical Reference Model
U.S.	United States
U.S.C.	United States Code
VA	Department of Veterans Affairs
VHA	Veterans Health Administration
VistA	Veterans Health Information System and Technology Architecture
VPN	Virtual Private Network
WBS	Work Breakdown Structure

ADDENDUM A

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed the VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Each documented initiative under this contract incorporates the VA Handbook 6500.6, "Contract Security," March 12, 2010, in its entirety. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses identified on the current external VA training site, the Employee Education System (EES), and will be tracked therein. The EES may be accessed at https://www.ees-learning.net/librix/loginhtml.asp?v=librix. Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). The VA reserves the right to assess contract deliverables for EA compliance prior to acceptance**.**

A2.1. VA Internet and Intranet Standards:

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is

not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser):
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser):
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A2.2. Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed are published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards:

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: http//www.section508.gov and http://www.access-board.gov/sec508/standards.htm. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as stated below:

- Technical standards from 36 CFR part 1194 Subpart B have been determined to apply to this acquisition. Solicitation respondents must describe how their proposed Electronic and Information Technology (EIT) deliverables meet at least those technical provisions identified as applicable in the attached Government Product/Service Accessibility Template (GPAT).

- Functional performance criteria from 36 CFR part 1194 Subpart C have been determined to apply to this acquisition. Solicitation respondents must describe how their proposed Electronic and Information Technology (EIT) deliverables meet at least those functional performance criteria identified as applicable in the attached Government Product/Service Accessibility Template (GPAT).

- Information, documentation, and support requirements from 36 CFR part 1194 Subpart D have been determined to apply to this acquisition. Solicitation respondents must describe how the information, documentation, and support proposed for Web Application deliverables meet at least those information, documentation, and support requirements identified as applicable in the attached Government Product/Service Accessibility Template (GPAT).

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the EIT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

A3.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. The VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. The VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A4.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of the VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of the VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.
2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment

wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.

6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by the VA.
7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    a. Controlled access to system and security software and documentation.
    b. Recording, monitoring, and control of passwords and privileges.
    c. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    d. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    e. Contractor PM and VA PM are informed within 24 hours of any employee termination.
    f. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    g. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

ADDENDUM B

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010

B1. GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

B2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

1. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.
2. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.
3. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.
4. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.
5. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is

reassigned or leaves the Contractor or Subcontractor's employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

B3. VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).
2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA's information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on-site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.
3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by the VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.
4. The Contractor/Subcontractor must receive, gather, store, back up, maintain, use, disclose and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations and policies. If Federal or VA information confidentiality and security laws, regulations and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.
6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.
7. If a VHA contract is terminated for cause, the associated BAA must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.01, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.
8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.
9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.
10. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor/Subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The Contractor/Subcontractor must refer all requests for, demands for production of, or inquiries about, VA information and information systems to the VA CO for response.
11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.
12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require C&A or an MOU-ISA for system interconnection, the Contractor/Subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

B4. INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, *VA Information Security Program*). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6507, *VA Privacy Impact Assessment*.
2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista) and future versions, as required.
3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.
4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.
5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.
6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.
7. The Contractor/Subcontractor agrees to:
    a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or

operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and
ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and
c. Include this Privacy Act clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

    a. "Operation of a System of Records" means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.
    b. "Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person's name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.
    c. "System of Records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as "Systems"), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems,

including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, based upon the severity of the incident.
11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to the VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes based upon the requirements identified within their contract.
12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure. Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.

B5. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

1. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA's network involving VA information must be reviewed and approved by VA prior to implementation.
2. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.
3. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires certification and accreditation (authorization)

(C&A) of the Contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (government facility or government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

4. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into VA's POA&M management process. The Contractor/Subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.
5. The Contractor/Subcontractor must conduct an annual self-assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The government reserves the right to conduct such an assessment using government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.
6. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on VA's network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of

approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

7. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to the VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.
8. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

    a. Vendor must accept the system without the drive;
    b. VA's initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or
    c. VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.
    d. Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for the VA to retain the hard drive, then;
        i. The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and
        ii. Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.
        iii. A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

B6. SECURITY INCIDENT INVESTIGATION

1. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.
2. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.
3. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.
4. In instances of theft or break-in or other criminal activity, the Contractor/Subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, and its Subcontractors and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The Contractor/Subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

B7. LIQUIDATED DAMAGES FOR DATA BREACH

1. Consistent with the requirements of 38 U.S.C. §5725, a contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract.
2. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data

breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

3. Each risk analysis shall address all relevant information concerning the data breach, including the following:
    a. Nature of the event (loss, theft, unauthorized access);
    b. Description of the event, including:
        i. date of occurrence;
        ii. data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
    c. Number of individuals affected or potentially affected;
    d. Names of individuals or groups affected or potentially affected;
    e. Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text;
    f. Amount of time the data has been out of VA control;
    g. The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
    h. Known misuses of data containing sensitive personal information, if any;
    i. Assessment of the potential harm to the affected individuals;
    j. Data breach analysis as outlined in 6500.2 Handbook, *Management of Security and Privacy Incidents*, as appropriate; and
    k. Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.
4. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to the VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:
    l. Notification;
    m. One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
    n. Data breach analysis;

o. Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
p. One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
q. Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

B8. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-days' notice, at the request of the government, the Contractor must fully cooperate and assist in a government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

B9. TRAINING

1. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
    a. Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the *Contractor Rules of Behavior*, relating to access to VA information and information systems;
    b. Successfully complete the *VA Cyber Security Awareness and Rules of Behavior* training and annually complete required security training;
    c. Successfully complete the appropriate VA privacy training and annually complete required privacy training; and
    d. Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access
2. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.
3. Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension

or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.